Analysis of Virtual Local Area Networking Technology

Zheng Zhang

Jiangxi Vocational and Technical College of Communication, Jiangxi, Nanchang 330013, China

123333@163.com

Keywords: VLAN; ISL; Ethernet; Networking Technology

Abstract. VLAN technology is widely used in construction and management of large-scale advanced network. With the wide use and development of VLAN, LAN networking becomes more flexible and convenient. In this article, we elaborate the working principle of VLAN, from the perspective of broadcast domain splitting and working across devices. And then we carry out analysis of the networking scheme of VLAN, and focus on the two widely used VLAN frame tagging methods, including IEEE802.1Q and ISL.

Introduction

In network applications, enterprise internal and external networks are separated by routers and firewalls. In order to ensure the security of the internal network, introducing virtual local area network (VLAN) technology is an effective way to coordinate and manage increasingly complex networks. Advantages of VLAN are to improve the efficiency of the network, to cut off from the network broadcast storms and to reduce broadcast traffic between different VLAN, so as to control the network maintenance costs. With the wide use and development of VLAN, LAN networking becomes more flexible and convenient.

VLAN is the end-end logical subnet constructed by network management software based on switched LAN, which can cross different segments and different networks. One VLAN is a logical broadcast domain. It is not limited by geographical position, and also can cover multiple network design. The switch that support virtual network can control broadcast traffic very well without routers. For LAN switch, each port can only mark a VLAN, and all ports in one VLAN has a broadcast domain, but ports in different VLAN can share different broadcast domains. Thus, the data transferred between computers in the same VLAN will not influence the computers in other VLAN. Actually, the switch acts as a router. Therefore, introduction of VLAN can effectively reduce the possibility of data exchange, so that avoid the broadcast storm, and improve the overall performance of the switched network and security.

The Working Principle of VLAN

Splitting broadcast domain. Broadcast domain is an important concept in LAN, which refers to a logical group of computers, and all computers in this group could receive the same broadcast information. Local area network (LAN) is usually defined as a separate broadcast domain, since it connects all nodes on the same network segment by hubs, bridges, or switches.

By VLAN division, it is able to split a large broadcast domain into several smaller broadcast domains. And each VLAN is a small broadcast domain. The principle is easy to understand, which is to limit the scope of the object MAC address “FF-FF-FF-FF-FF-FF-FF” to the current VLAN, and do not to transmit to others. For example, if there are 1000 computers originally in a large

VLAN, and one of the computers can send about 10KB broadcast data in a second, so the total amount of traffic is up to 1000*10KB, which due to the broadcasting.

By VLAN, we can segment broadcast domain, and it also brings security highly improved. For lots of network security problems such as ARP deception, network sniffing, network scanning act, all use broadcast packet, after VLAN division, the network security problems will limit to the scope of VLAN, could not attack other VLAN anymore.

Working across multiple switches. The division of VLAN is carried out on the switch generally, and one VLAN can not be defined in one switch, it can work across multiple switches. As you can see in picture below, there is VLAN, each VLAN across two switches, and one of the VLAN is access port, the two switches allow all VLAN across, and it usually called trunk port.

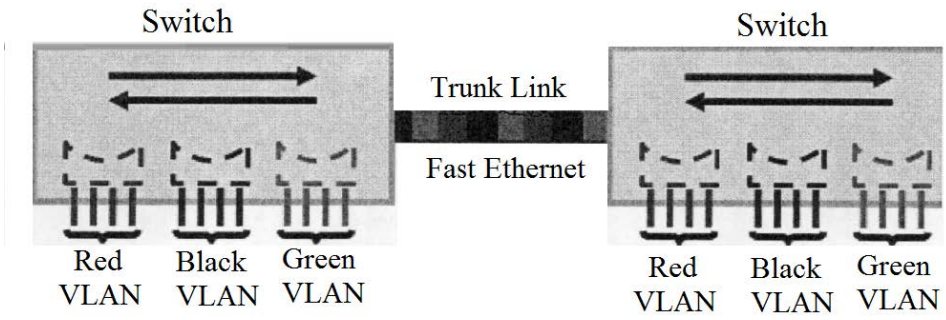

Fig. 1. VLAN on several switches

One of the goals of the VLAN is to build a working group model. The concept is: after fully implementation of the VLAN in a network across campus, same department or segment can share VLAN, and the large part of network flow remains in the same virtual VLAN inner. On the opposite side, if user changed, no need to change his/her actual position, only the network administrator needs to change the user's virtual VLAN member.

In campus network, VLAN work across with multiple switches, so the division of VLAN would not be effected by physical positon. If one department located in separated buildings, it can combine the switch with one VLAN.

The Networking Scheme of VLAN

The scheme of VLAN implementation is mainly up to insert sign in data frame. VLAN works on the second layer: data link layer. In this layer, the unit of date transmission is frame. The common Ethernet frame format is shown as follow:

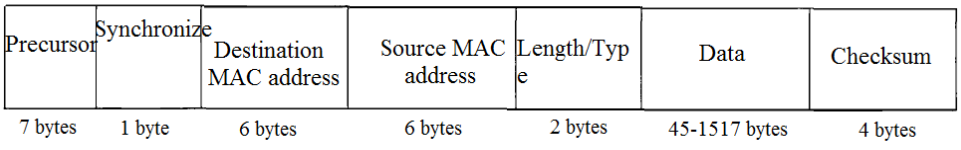

Fig. 2. Format of the Ethernet Frame

As above Fig. 2, the frame conclude source address, destination address, frame date, calibration, and other fields, the frame sign not included, so it cannot separate one frame from others. For conclusion, there needs adding a unique VLAN sign in date link layer. In practical applications, the widely used VLAN frame tagging mainly includes the following two methods:

IEEE802.1Q. Before being sent to inter-switch link, the head of Ethernet data frame will be repackaged, to reflect some certain VLAN ID. Then when it is sent to Terminal Equipment, the head will be converted back to the original format. The IEEE 802.1Q protocol stipulates for a period of new Ethernet frame field, as shown in Fig. 3:

Precursor	Synchronize	Destination MAC address	Source MAC address	802.1Q header		Length/ Type	Data	Checksum
				TPID	TCI			
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	2 bytes	2 bytes	45-1517 bytes	4 bytes

Fig. 3. Format of IEEE 802.1Q Frame

Compared with the head of standard Ethernet frame, VLAN packet format increases a 4 bytes 802.1Q tag, which contains 2 bytes tag protocol identifier (TPID) and 2 bytes tag control information (TCI). TPID is a new type defined by IEEE, and its value is 1000000100000000, indicating it is a packet with 802.1Q tag. The specific format of 802.1Q header is shown as Fig. 4:

TPID--Tag Protocol Identifier		**TCI--Tag Control Information**		
10000001	00000000	**Priority**	**CFI**	**VLAN-ID**
Byte 1	Byte 2	Byte 3		Byte 4

Fig. 4. Format of IEEE 802.1Q header

The information in the tag header can be interpreted as:

a) VLAN identified: it is a 12 bit field. All the data pack sent out from every computer that supports 802.1Q protocol will contain this field, to demonstrate the belonging VLAN.

b) Canonical format indicator (CFI): it is mainly the frame format used in data interchange between bus Ethernet and FDDI.

c) Priority: there are a total of eight priorities. When the switch is blocked, the data packet of high priority will be sent preferentially.

Inter-Switch Link (ISL). ISL is a protocol that transfers VLAN information and VLAN data flow between switches, switch and router, switch and server. By configuration of ISL package with the directly connected port in switch, VLAN assignment and configuration of the entire network could be achieved.

ISL frame is mainly composes of three parts: header, original Ethernet frame and frame check sequence (FCS) in tail. The ISL package is added to the Ethernet data frame for 30 additional bytes, but don't modify original Ethernet frame. When the frame is forwarded to the port of the trunk link, VLAN ID is added to frame; when frame peel off the port of the trunk link, ISL package will be removed. The format of the ISL frame is shown in Fig. 5:

DA	**TYPE**	**User**	**SA**	**LEN**	**SNAP/ LLC**	**HAS**	**VLAN ID**	**BPDU /CDP**	**INDX**	**Reserved**	**Original Frame**	**FCS**
40 bits	4 bits	4 bits	48 bits	16 bits	24 bits	24 bits	15 bits	1 bit	16 bits	16 bits	variable	32 bits

Fig. 5. Format of the ISL frame

(1) Destination address DA: multicast address, set as 01. 00. 00. 00. 00, and inform the receiver this is an ISL frame.

(2) Frame type TYPE: indicates the type of frame being encapsulated. The encoding meaning is:

0000: Ethernet;

0001: token ring;

0010: FDDI;

0011: ATM.

(3) User defined bits USER: for Ethernet, User domain bit 0 and 1 indicate the priority that data package via switch. The encoding meaning is:

00: normal priority;

01: priority 1;

10: priority 2;

11: highest priority.

(4) Source address: it is 802.3 MAC address of the switch port sending data frame, 48 bits.

(5) Length LEN: it represents the length of data package, excluding the length of DA, TYPE, SA, LEN, and CRC domain.

(6) SNAP/LLC: it is a constant 0X AAA03 of 24 bits.

(7) High bit of source address HAS: it is 3 bytes in SA domain, representing the ID number of MAC manufacturer.

(8) VLAN ID: it refers to the ID number of VLAN which data package belongs to, 15 bits in total, and it can be used to distinguish between different VLAN frames.

(9) BPDU/CDP indicator: it is called bridge protocol data unit, which is used by VLAN spanning tree algorithm to determine the information about topology.

(10) Indexes INDX: it indicates the data packet source port index when data package exits the switch, for the purpose of diagnosis.

(11) Reserved domain: it is used for FDDI and ISL encapsulation. For Ethernet frame, all the value of this domain is 0;

(12) Encapsulated frame: length of original frame is variable from 1 to 24575 bytes, containing Ethernet frame, FDDI and token ring data frame. When the receiver removes the ISL encapsulation, this domain will be taken as the received frame.

(13) Frame check sequence FCS: FCS is CRC value of standard 32 bits, which can launch calculation and frame check sequence on the encapsulated frame.

ISL and IEEE802.1Q are both explicit labeling, indicating that it is explicitly tagged with VLAN information. However, their labeling mechanisms are different. IEEE802.1Q uses the internal labeling process, that is, modify the existing Ethernet frame with VLAN identification, and it still appears in the form of standard Ethernet frames, so IEEE802.1Q frame can appear on the access link and the trunk link at the same time. On the contrary, ISL protocol is a kind of external labeling process. ISL encapsulates the ISL header with 26 bytes, instead of modifying the original frame. Meanwhile, an additional 4-byte FCS is added at the end of the frame, which means only the devices support ISL could interpret this frame.

References

[1] Zhao L F. Exploration and Practice for Virtual Local Area Network (VLAN) Technology[J]. Applied Mechanics & Materials, 2012, 241-244:2299-2302.

[2] &Lt B W, Net&Gt B. Textual Conventions for Virtual Local Area Network Identifiers (VLAN-ID)[J]. Saber Revista Multidisciplinaria Del Consejo De Investigación De La Universidad De Oriente, 2009, 21(4):312-317.

[3] Amin M R. Analysis on the Virtual Local Area Network to Reduce Collision Domain and Manage Broadcast Domain[J]. Asian Journal of Information Technology, 2007(10).

[4] Qin C H, Wang N, Ren H D, et al. Simulation and study on data communication in digital substation based on virtual local area network[J]. Power System Protection & Control, 2013.

[5] Mittal A, Chen H P. PRIVATE VIRTUAL LOCAL AREA NETWORK ISOLATION[J]. Cisco Technology Inc California, 2014.